World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Cybersecurity leadership policy and compliance for institutions of higher education

Bradley Fowler *

Dissertation Chair, Capitol Technology University, 11301 Springfield Rd., Laurel, MD 20708, United States.

World Journal of Advanced Engineering Technology and Sciences, 2024, 12(02), 553–563

Publication history: Received on 23 June 2024; revised on 31 July 2024; accepted on 02 August 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.12.2.0331

Abstract

Cybersecurity pairs with information asset storage and security for institutions of higher education. When institutions of higher education lack effective cybersecurity leadership, cyber incidents escalate. Worldwide, institutions of higher education are experiencing threats and vulnerabilities woven in their information systems and technology applications. This requires strategic resolutions. One strategy is cybersecurity and information security policy. Research collected worldwide proves usage of cybersecurity policy aligned with federal international law, establishes a cyber culture of compliance. Furthermore, personnel, internally and externally, are the bridge to managing access to data assets, and unless they are knowledgeable of the policy mandated by the institution and its cybersecurity infrastructure, the results of non-compliance can be catastrophic. Since the United States National Institute of Standards and Technology enacted cybersecurity policy for federal information systems. Institutions of higher education must adhere to these standards and guidelines to manage threats and vulnerabilities programmed in their hardware, software, and cloud. Therefore, why are so many institutions of higher education neglecting to align policy and enforcement of policy with these standards? What problems are creating non-compliance among institutions of higher education personnel and executive leadership? How can cybersecurity leadership improve policy and compliance to control risks factors programmed in information systems, technology, and cloud applications, institutions of higher education rely on to reduce human error? To assess and answer these questions, the researcher deployed qualitative grounded theory lite research to assess trends of cybersecurity leadership at institutions of higher education and to improve policy development and compliance.

Keywords: Cybersecurity leadership; Cybersecurity policy; Cybersecurity at institutions of higher education; thwarting cyberattacks; Higher education policy compliance; Cyber policy for higher ed

1. Introduction

The United States National Institute of Standards and Technology is responsible for developing and implementing information security standards and guidelines for federal information systems. Under NIST SP 800-53 Rev. 5- Security and Privacy Controls for Federal Information Systems and Organizations, authored by Joint Task Force, published in December 2020, all non-federal organizations are encouraged to mirror information security standards outlined in FIPS Publication 200, Minimum Security Requirements for Federal Information Systems [1]. Furthermore, in FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, non-federal entities are encouraged to configure their security levels with the appropriate security baseline controls to help decrease risks factors commonly exploited by cybercriminals. Adherence to these standards has proven valuable to decreasing the number of successful cyberattacks deployed against federal information systems. However, not much research is currently available reporting the success rate of usage by non-federal entities, to determine the reliability and validity of these standards as primary controlling factors in reducing successful cyber-attacks. What is published to support these standards as reliable and valid, are technology industry related reports published in bias content from experts across the information systems and technology profession, who strongly advocate for usage and integration of

* Corresponding author: Bradley Fowler ORCID: 0000-0002-8447-7898

these standards to support cybersecurity efforts. Since institutions of higher education are partnered with the U.S. Department of Education and receiving federal grants (i.e., Pell and Federal Supplemental Educational Opportunity Grants) as well as private loans (i.e., Grad Plus), institutions of higher education are highly recommended to align their development of cybersecurity leadership strategies and activities with these standardizations to deter and decrease cyberattacks. However, the growth of cyberattack incidents reported in the United States and globally, incites alarming awareness invoking interest in how many institutions of higher education are neglecting to improve their cyber resilience and mitigation efforts as outlined in these standardized guidelines.

Research reports the number of cyberattacks deployed against institutions of higher education has grown 55% more in 2023 compared with attacks deployed in 2019, when such attacks began making news headlines. The growing phenomenon of cyberattacks against institutions of higher education is impacting the ability for many institutions to thwart these attacks successfully, resulting in reputational damage, decrease in enrollment, and causing some institutions to close their doors. Research compiled from IBM shares details confirming the education sector is a frequent target. IBM conveyed the education sector experienced the 11th highest data breach cost out of 17 sectors [2]. Institutions that rely on third-party large data transmission services rendered by MOVEIt were greatly impacted. The cost of these attacks reached one million dollars. Research also reports that 74% of cyberattacks targeting institutions of higher education have been successful [3]. Moreover, research reports that within a month time during spring 2022, institutions of higher education were the target of more than 6.1 million malware attacks. And if this is not enough to invoke concern regarding current trends in cybersecurity leadership in this sector; research also reports that institutions of higher education are held accountable to fierce federal laws and policy that often result in steep fines and litigation, including civil complaints. Federal laws include protection of personal student data, financial information, academic research, clinical research, and government research. Thus, institutions of higher education must take improved actions to update efforts to development effective cybersecurity leadership that controls risk factors through risk management framework and executive leaders and personnel compliance with mandated cybersecurity policy. In doing so, institutions of higher education can begin to gain control over their potential threats and vulnerabilities and upgrade mitigation efforts that place full control over information assets, into the hands of cybersecurity leaders who take charge in defending institutions of higher education information assets stored in information systems, technology hardware, software, and cloud engineering.

To achieve optimal performance, it is important for institutions of higher education to understand three things. First, it is important to understand why are so many institutions of higher education neglecting to align their policy development and enforcement with federal standards and guidelines outlined in NIST SP 800-53 Rev. 5? Secondly, it is important to understand what problems are creating cybersecurity policy non-compliance among institutions of higher education, personnel and executive leadership? And the third most important question is understanding how can cybersecurity leadership improve policy and compliance to control risk factors programmed in information systems, technology, and cloud engineered applications to reduce human error? To deploy effective research to gain answers to define a resolution for these three research questions, required the researcher to use qualitative grounded theory lite research. This approach is unlike grounded theory introduced by Barney Glaser and Anselum Strauss, who are considered founding fathers of this research method. Glaser and Strauss believed this approach to research is rooted in methodological traditions of inquiry, deployed to explore a social or human problem [4]. This research process develops a complex assessment of words and shares details of collected information to deploy the study in a natural setting. This research is defined by observation and interpretation of people's perception of various events and evaluates those perceptions to define a new theory of perception. This approach allows the researcher to derive at a theory and revise that theory into another theory to compare and contrast theory that builds a new theory that can then invoke an increase of developed theory. Unlike qualitative grounded theory, qualitative grounded theory lite research does not depend on a theory being developed. This approach is best used when the research scope is smaller and does not require reliance on the development of a theory [5]. Thus, the researcher chose this research method to answer these three research questions.

2. Literature Review

The Joint Task Force Transformative Initiative has become a vital asset in the United States Department of Commerce National Institute of Standards and Technology, towards the development and introduction of standardized procedures and processes that are invaluable to public and private sector entities, utilizing information systems, technology, and cloud computing and engineering for business operations and communication, to develop, retrieve, share, store, and secure information assets. Utilization of several published special publications categorized under the 800 series, plays a key role in helping convey the significance for reliance on these publications and reason for partnering with this public service entity, who has become instrumental in rendering standards in controlling risk factors associated with usage of information systems, information technology, and cloud computing and engineering. Adopting the standards promoted

through these 800-series publications has become a vital method of managing and controlling risk factors woven into public and private sector. The researcher has adopted standards from these publications to improve current trends in cybersecurity leadership at institutions of higher education. This research provides the methodology of doing so.

Since inception, the grounded theory research model has become beneficial for creating a new theory from comparison and contrasting data. Utilization of key details shared by researcher Shahid Khan in his published article, enables the researcher to convey his decision to utilize grounded theory lite research for this article. Although the researcher is utilizing grounded theory lite research, a less time-consuming method that does not require establishing a new theory. Sharing the procedures of grounded theory, including open-coding, axial coding, and selective coding, helped the researcher utilize this research model to meet the needs of this research study and answer the research questions to establish a resolution to this phenomenon.

Published blog content from subject matter expert Emily Miller, writer for BitLyft, reports the state of higher education cybersecurity trends, helps the researcher clarify what issues are impacting institutions of higher education in thwarting and deterring cyberattack incidents. This article conveys concerns many institutions of higher education share and provides statistics that impact the need for improved cybersecurity leadership. This article increases awareness and outlines weaknesses institutions of higher education embody within information systems, information technology, and cloud computing and engineering, responsible for storing and securing information assets. Usage of this content enables the researcher to validate his purpose for deploying this research study as a qualitative grounded theory lite study. Furthermore, usage of blog content published by Delve & Limpaecher, enables the researcher to align his research with standards of grounded theory coding utilized in grounded theory research. This resource is instrumental in supporting the researcher's research method and decision to utilize grounded theory lite, as his primary concept of this research. This resource also validates the grounded theory lite method as an effective way to answer the researcher's research questions.

In addition, a scholarly article titled Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance, was instrumental in helping the researcher effectively assess the human behavior of workplace personnel in alignment with compliance and noncompliance behaviors. This article also enabled the researcher to grasp some clarity regarding the suggested deterrence techniques, management behaviors, and organizational culture that also impacts the ability for noncompliance behavior to transition into compliant behavior. The researcher believes this article is valuable because it validates grounded theory lite research correlating with the resolution, the researcher shares in this article.

Finally, the researcher discovered an article titled Information security policies: A review of challenges and influencing factors, which was essential in supporting the development and implementation of information security policies that work. Higher education institutions differ greatly in size, demographics, culture, and infrastructure, as well as the scope of technology reliance they share. Unless there is riveting evidence supporting the need to enforce information security policy, this subject is often overlooked. Yet, this article provided the clarity regarding the significance of information security policies and reinforces the importance of developing clearly conveyed policies that can support each individual institution of higher education, towards achieving 100% compliance, to help deter and thwart successful cyberattacks. In doing so, these institutions can increase effective cybersecurity leadership.

2.1. Method of Data Collection

Utilization of EBSCO Host, ProQuest, Google Scholar, Google, Lukol, Bing, Dogpile, Duck Duck Go, and additional search engine platforms, including Science.gov, Research Gate, and Science Direct, supported the researcher's quest to acquire a minimum of 30 scholarly published documents supporting the topic of this research and the research method utilized to define results that are instrumental in rendering an effective resolution to integrate cybersecurity leadership strategies, institutions of higher education can rely on, to secure their hardware, software, technology applications, tools, and cloud. Keywords utilized to acquire documents in PDF file format, Web page content, and Blog content delivery, included cybersecurity leadership, cybersecurity policy, cybersecurity at institutions of higher education, thwarting cyberattacks, higher education policy compliance, and cyber policy for higher ed. Cross reference of data assets also derived from additional databases correlating with U.S. Department of Homeland Security, Cybersecurity Infrastructure & Security Agency, and the National Institute of Standards and Technology. Peer reviewed scholarly published journals provided statistics collected from IT and cybersecurity practitioners working at institutions of higher education in the U.S., Europe, and Middle East. Because the researcher is utilizing qualitative grounded theory lite research, the researcher is not required to formulate a theory from the data collection. Instead, the researcher utilizes the data collection to consistently compare and contrast concepts of theory enveloped in all documents compiled to

help prove his theory that cybersecurity leadership at institutions of higher education must improve development, implementation, and reliance of cybersecurity policy, to become an effective method of deterrence.

3. Research Method

In 1967, Barney Gallard Glasar and Anselm Leonard Strauss developed the grounded theory method from data relying on open concepts and ideas they collected from that data. The goal of grounded theory is to theorize and cultivate meaning of the lived experiences of people in society. The researcher chose this research method because it enables him to theorize reasons institutions of higher education neglect to adhere to standardized policy mandated by federal and international law, regarding the governance of information security assets, as well as the utilization of cybersecurity policy. Penalties for noncompliance with federal law regulating information security of federal information systems and federal information systems hosting information, including student financial aid information, student social security numbers, dates of birth, medical records, and private banking information, fall under the Family Educational Rights and Privacy Act and Protection of Pupil Rights Amendment, which can result in a withdrawal of federal funding provided by the U.S. Department of Education. Reliance on federal funding at institutions of higher education, domestically, accounts for 72% of undergraduate students who received some level of federal financial aid to cover the cost of tuition. Seventy-four percent of graduate students in the United States received some financial aid in 2019-2020 [9]. These numbers account for up-to 100% of institutions in America. Therefore, American institutions of higher education are accountable to these federal laws.

Using grounded theory lite, the researcher can assess scholarly published, peer reviewed documents reported by the United States Department of Education and public and private institutional reports and databases, regarding the number of cyberattack incidents that occurred during the 2019-2023 school years [10]. What the researcher learned through a Google search query using keywords: cyber-attack incidents at higher education 2019-2023; populated a return of one-million results including Web pages, forums, and videos of data collection to gain clarity on the scale of institutional cyber-attack incidents. These reports convey, in part, that ransomware attacks are up 75% across public and private institutions and cyberattacks cost an average of $740,000 U.S. [11]. Populated resources also report that higher education data breaches cost an estimated $3.5 million on average in 2023 [12]. Furthermore, it is reported that 1500 U.S. institutions of higher education operate an average 244 domains. The top 450 institutions of higher education own an average of 600 domains, and the top 90 institutions of higher education have an average of 1500 domains [13]. Domain represents Domain Name Servers (DNS), relating to IP addresses relied on by these institutions to transmit data across the Internet.

Using open coding from grounded theory, the researcher assessed the collected information to create a theory that institutions of higher education in the U.S. operate a large volume of domains that increase risks factors leading to cyberattacks. When domain name servers (DNS) are vulnerable, they can be exploited by external and internal attackers. Research explains that institutions of higher education have large attack surfaces that enable cyber attackers to gain access to vital information, compromise systems, or lock out end-users. The attack surface at institutions of higher education has grown complex due to domain networks, because this creates a large scale of network entry points that are easy to exploit [14]. When open coding is applied, the researcher assessed what type of cyber incident is commonly deployed at institutions of higher education that resulted from these exploitations, including Distributed Denial of Service Attacks, ransomware attacks, malware attacks, SQL injections, viruses, and Trojans. Phishing attacks, email phishing attacks, and executive whaling attacks are common among internal human error incidents that enable external attackers access to the network via a simple error in judgement demonstrated by personnel or an executive leader. Human error is reported to account for 85% of all data breaches, in both public and private sectors.

Axial coding enabled the researcher to outline a comparison of cyberattack incidents and methods occurring at institutions of higher education, as they relate to the type of attacks deployed at each individual institution. Using grounded theory lite enabled the researcher to exclude relying on large scales of research data and conclude his theory that institutions of higher education are experiencing domain exploitation, because their information systems and technology usage across their networks are ineffectively configured and absent cybersecurity leadership auditing processes and policy practice, that govern how these systems are regulated, updated, backed-up, archived, and secured. These are primary risk factors that lead to security breaches.

Grounded theory selective coding is significant because this process enables the researcher to finalize his theory and report validating evidence that his theory is accurate. Using qualitative grounded theory lite, does not require the researcher to ensure research collected is reliable to support a theory, because no theory must be established. What the researcher hoped to establish are valid facts that many institutions of higher education neglect to align their policy development and enforcement with federal standards and guidelines outlined in NIST SP 800-53 Rev. 5. After all, this

policy requires effective security and privacy controls for information security and privacy management [15]. Therefore, this approach to qualitative grounded theory lite validates the researcher's first question with a clear answer. After all, it has been reported since 2019, that institutions of higher education are collectively neglecting to implement effective cybersecurity leadership that governs usage of information systems as a storage capacity for data assets. This results in increased risk factors that are now being easily exploited because reports prove institutions of higher education are easy targets and willing to pay ransomware costs.

All three grounded theory methods of data collection (i.e. open coding, axial coding, and selective coding) are key steps to support the proposed theory that when cyber security leaders adopt effective alignment with mandated federal law and policy, regulating information systems, information technology, and cloud computing and engineering, a scale of leverage is established that reduces the impact a cyberattack has on an institution. Regardless of the initiative to remain compliant with NIST SP 800-53 Rev. 5, or any other mandated regulation; institutions of higher education are grappling to maintain control over the risk woven in software, hardware, and technology tools and devices, that store and transmit sensitive data assets. To improve this problem requires a firm resolution that will impact change that cannot be reversed.

In addition, to answer the question what problems are creating cybersecurity noncompliance among institutions of higher education, personnel and executive leadership, research compiled using grounded theory lite document collection, helped the researcher explain that an estimated 90% of large organizations and 55% of small organizations are considered to embody and rely on documented information security policy [16]. In fact, research reported by E&Y global information security survey, reported that 57% of organizations believe their employees actions and behavior can result in cyberattack. 35% of organizations reported that carelessness and unawareness of policy regulations increase cyberattack threats. In the UK, it is reported that security policy noncompliance accounts for 70% of organizational breaches [17]. Thus, many organizations agree the rate of human incidents that cause security breaches increases the number of successful cyberattacks. Grounded theory lite enables the researcher to report that ineffective usage of cybersecurity policy leads personnel to engage in behavior that is ignored and results in common exploitation of information systems. When organizations develop information security and cybersecurity policy that is shared across the organization, that is provided via effective awareness training, and employees' are in compliant with practicing policy applications, there are greater chances the number of successful attacks is reduced substantially. Research reports that four commonly shared issues across organizations correlating with information security policy challenges, include promotion of the organization's security policy, non-compliance with security policy, security policy management, and unclear and ineffectively written security policies. Grounded theory lite also enabled the researcher to understand factors that influence human behavior resulting in security breaches, including internal low-quality of data exchange, lack of individual motivation, ineffective awareness training development, implementation, and assessment, monitoring of computer systems, and ineffective ability to persuade compliance.

Thus, this research method is a reliable way to determine what resolution can best serve the needs of institutions of higher education, in assessing the lack of motivated compliance shared across all employees', to understand methods of compliance infrastructure to deploy. This research method also enabled the researcher to define a resolution that clarifies what steps should be taken to ensure institutions of higher education are ensuring significant practice be implemented to ensure network ports are secure on all domains and networks are audited to ensure policy compliance and alignment that meets the demands of federal laws and policy, to protect and secure students, faculty, and executive leaders sensitive information. Most importantly, this research method provides validity that supports its purpose and benefits institutions of higher education, by contributing knowledge to support the lack of understanding relating to the steps needed, to implement effective cybersecurity leadership through usage of cybersecurity and information security policy.

This research method also enabled the researcher to answer the question regarding how cybersecurity leadership can improve policy and compliance to control risk factors programmed in information systems, technology, and cloud applications, as well as to reduce human error. This was achieved through a comparison of non-information security policy usage in 50% of U.S. institutions of higher education. And 50% of cybersecurity policy usage in institutions of higher education in Saudi Arabia. This research reports that in 2024, U.S. higher education institutions are investing in cybersecurity policy development, implementation, and reliance on this regulatory framework more, to ensure improved cybersecurity leadership. But how effective will this be? After all, unless there is a federal or state agency that follows-up and audits these institutions, not every institution of higher education in America will be effective in deploying this strategy.

When examining the implementation of cybersecurity leadership implemented in institutions of higher education in Saudi Arabia, research explains that cybersecurity has propelled towards significant value in national security, invoking

increased investment in technologies that protect information assets, deter threats, and preserve privacy. Research also conveys that although reliance on the Protection Motivation Theory is present, it is believed that assessing the performance of cybersecurity policies and measure (threat appraisal) is vital for effective usage (coping appraisal). Additionally, a study was deployed on cybersecurity experts working at institutions of higher education in Saudi Arabia. Participants included 10 representatives from various colleges and universities and 107 respondents, who participated in a survey utilizing questionnaires and interviews to collect data. The outcome of this research proves there is a need for increased improvement of cybersecurity leadership across all Saudi universities. Despite a few respondents reporting regular risk assessments are deployed timely enough to identify risks. Many research participants conveyed sincere concern regarding the lack of policy usage and availability of standard procedures. There is also a high volume of respondents who believe insufficient training and awareness programs play a role in the increased number of cyberattack incidents. While non-compliance with cybersecurity policy regulations and standards remains a norm.

In addition, this research reports that an estimated 40% of institutions of higher education in Saudi Arabia have not developed and implemented adequate cybersecurity policy. While 50% reported their institution has implemented effective cybersecurity policy that is proving useful in supporting their institution in lowering their cyber risk factors. How effective can cybersecurity policy be in one country but not effective in all countries, institutions of higher education. The grounded theory lite method shows beneficial in answering this question, because the consistent comparing and contrasting of data assets through open-coding, axial-coding, and selective coding grounded theory methods, enables research collected from the United States, Europe, and Middle East institutions of higher education, to enable the researcher to convey a resolution to improve the estimated number of institutions of higher education, worldwide, towards thwarting cyber-attack incidents. The researcher shares his results of this grounded theory lite research study below.

4. Results

Qualitative grounded theory lite research method provides substantial results collected from 10 peer reviewed scholarly journal articles that report substantial evidence that cybersecurity policy and information security policy are absent tools that can be useful in supporting institutions of higher education thwart and deter successful cyber-attack incidents, and in lowering human error. When cybersecurity policy and information security policy are paired, these two regulations can play a significant role in governing high level risk factors woven in usage of vulnerable information systems, technology, hardware, and software applications. The alarming scale of ineffective development of cybersecurity and information security policy at an estimated 60% of institutions of higher education across the United States, can increase the number of reduced cyber incidents. Usage of peer-reviewed evidence from CoSN Leading Education Innovation, a non-profit organization responsible for publishing a research report funded by Bill & Melinda Gates, focusing on current and aspiring K-12 education technology leaders, and disseminating knowledge and professional development required to create and develop engaging learning environments, reports that a recent Government Accountability Office (GAO) report shared that a cyberattack impacts the loss of learning among students between 3 days and 3 weeks after the incident occurs [18]. Furthermore, it reports that recovery can take up to 2 to 9 months. This report conveys, in part, that to decrease and slow the growth of cyberattacks will require innovative resolutions and increased collaboration among education leaders and policy makers at every level of government.

The results of qualitative grounded theory lite research shows that inconsistent compliance among institutions of higher education in aligning their usage of information systems security policy, regarding how to store information assets, increases the risk of vulnerabilities in these systems, making it easier for cyber criminals to deploy successful attacks. The assessment of the above report also conveys that the increased number of education cybersecurity bills introduced by state legislators grew to more than 250% and the number of new legislative laws adopted by states grew beyond 600%. As a result, many state leaders have not only initiated increased focus towards cybersecurity needs of the education sector, to increase the awareness and adoption of a broader scope of policy strategies, including developing cyber risk insurance funds, creating regional alliances and partnerships, and providing scholarship programs to expand cybersecurity partnerships. Shockingly, it is also reported that Congress has been less instrumental than states regarding educational cybersecurity policy throughout 2023. Even though federal agencies, such as the Federal Communication Commission and the Cybersecurity and Infrastructure Security Administration propose to increase actions to support schools to improve their cyber defense. The results of qualitative grounded theory also proved that institutions of the United States, Europe, and Middle East are all wrestling to understand the role cybersecurity leadership and policy can have on managing cyber risk factors and reducing malicious cyber-attack incidents. However, the collected documents prove that the commitment to develop, integrate, and improve usage of cybersecurity policy and information security policy at higher education institutions, unless enforced, remains highly ineffective. Non-compliance results from human behavior that is not being assessed, evaluated, and understood, to increase focus on improving integration of cybersecurity policy as a driving force to control increased threats and vulnerabilities. The

reported mass of institutions who have been victimized by cyber-attack incidents from 2019-2023, as reported in this collection of documents the researcher relied on, proves there is a vital need to increase development of policy that aligns with federal and international cybersecurity law and policy. Furthermore, it is proven ineffective awareness and training regarding cybersecurity policy and information security policy in institutions of higher education, continues advocating for human error incidents to occur and often be ignored and never penalized. This too, advocates for cybercriminals to deploy attacks that include ransomware, malware, Denial of Service Attacks, phishing attacks, and SQL injections.

The comparison of documents collected from 2019-2024 also proves there remains a wide absence of resolution in adopting cybersecurity policy that aligns with federal law and policy, to improve the compliance of personnel in institutions of higher education, to help manage the consistency in compliance with policy requirements. Research reported in data collection also proves that information security policy compliance is a human behavior issue. And although usage of psychology has become useful, this approach has not rendered a reliable response providing this method is the best way to ensure compliance. As the researcher continued developing a new theory and ensuring such theories were applicable, the researcher was able to define clear recommendations to conclude the need to continue the growth of contribution of knowledge towards understanding this central phenomenon, and how to manage the threat of cyber-attacks targeting higher education. Thus, the researcher shares recommendations and a conclusion.

5. Discussion

In the cry of a storm, people panic and often neglect to recall methods, procedures, and processes that were provided during training. Despite the environment there is a need to reinforce policy that is reliable and demands respect and compliance from everyone held accountable. Within institutions of higher education where cybercrime and cyberattacks are growing more prevalent, reliance on cybersecurity leadership is invaluable to the security of the information systems, information technology, and cloud relied on to secure information assets. In fact, research conveys that an estimated 68% of cyberattack incidents occur due to human negligence, either intentional or unintentional. In a study deployed using security professionals' behavior, it was concluded that an estimated 40% of data breaches are caused by employees' behavior [6]. Research also conveys that in 2014 IBM utilized a cybersecurity intelligence index to report an estimated 90% of information security incidents engulf some level of employee negligence [7]. Thus, a driving force of malicious activities in the workplace are driven by attackers, who target employees' inconsistent compliance with workplace policy.

Clearly, this shows a demand for increased reliance on a policy infrastructure that can be enforced and complied with to enable institutions of higher education to improve their goal of lowering cyberattacks. Although usage of information security policy alone is not enough to guarantee adherence and compliance. Unless information security policy become a driving force to ensure cybersecurity leadership is top priority, there will remain a negligence in policy compliance. But why does policy noncompliance exist when workplace personnel and employees' are made aware of the value of these initiatives. The alarming number of cyberattack incidents at institutions of higher education should be enough to invoke all higher education institution employees' and personnel, to adapt effective compliance with limited issues. However, research reports policy compliance is a human behavior concern many organizations are facing. Concerns tend to envelop issues closely relating to a lack of educational training, which often is ignored because those implementing the training do not effectively assess those being trained. This leads to inconsistency of compliance. Moreover, research explains that studies report stress, work impediment, and coworker behavior impact employees' behavior. While this features some of the issues, this does not provide a full scope of the problem.

Researchers have tried utilizing psychological factors to determine the core fabric of issues that lead to policy noncompliance and human behavior negligence. However, these studies remain insignificant in providing a clear understanding of problems that can relate to all information security policy noncompliance issues. What has become useful through these research studies, to effectively assess human behavior that correlates with understanding what invokes noncompliance and compliance with information security policies, is that this is a difficult subject to assess, as well as understand the correlation between those who willfully comply with information security policy and those who do not. Thus, the researcher believes each institution of higher education must design their own approach to improve policy development, implementation, assessment, accountability, and penalties for noncompliance. Otherwise, the focus on information security policy remains insignificant to controlling the human behavior known to enable successful cyberattacks to occur.

The researcher believes to achieve optimal performance in alignment with institutional information security policy, requires defining strategies that enforce consistency in human behavior that aligns with each institution of higher education information security policy. While it is recommended to configure policy with NIST special publications.

Additional recommended policy infrastructure alignment includes ISO/IEC 27001/27002, which is developed and offered by the International Organization for Standardization and the International Electrotechnical Commission. The ISO has been instrumental in rendering international standards for information security management systems since 2005. This organization delivers details regarding the SOC 2 assessment report, that helps organizations achieve improved compliance. This cybersecurity audit process has become rapidly utilized across various organizations to invoke a sincere interest in cybersecurity leadership and privacy issues organizations have. Reliance on the SOC 2 audit enables an organization to review their policies, procedures, and systems across a five-category scope called Trust Services Criteria (i.e., Security, Availability, Processing Integrity, Confidentiality, and Privacy) [8].

This can be a benefit for the researcher's research study when applying qualitative grounded theory lite, because the researcher can assess the number of organizations that utilize this approach to assess the potential benefits this system can render to institutions of higher education. Because the researcher is utilizing qualitative grounded theory, it is imperative to collect lived experiences of cybersecurity leaders correlating with institutions of higher education. Then the researcher can begin to code the collected data in the three-step process associated with traditional grounded theory research (i.e., open-coding, axial-coding, and selective coding). In doing so, the researcher can prove his theory that cybersecurity leadership can help decrease the growing threat of cyber-attacks at institutions of higher education, when policy is developed effectively, implemented correctly, end-users are assessed and trained, and reassessed quarterly, to enforce a consistency in compliance that impacts the rate of cyber incidents each institution experiences.

6. Conclusion

Collaborative communication is a must among institutions of higher education to gain clarity on the type of cyber-attack incidents experienced and being deployed. When communication is shared, it enables everyone to understand what they are facing and gain some idea of what was deployed by the victim, to integrate and mirror those actions in their own strategy. Thus, an open-source incident reporting site must be established and effectively managed. This network can be a government established entity or a public university system and/or private. The scope of institutions across regions, domestic or international, requires the same scale of cybersecurity leadership and policy development and implementation. This entity can also be a network deployed by a non-profit entity, who mediates communication sharing and provides analytic reports, research on cyber-attack incidents, level of risk being discovered across institutions, database files of suggested mitigation strategies, methods of management, and a forum for discussion regarding laws, policy, and bills under review regarding cybersecurity leadership and policy development and integration for higher education institutions.

It is recommended higher education adopt improved methods of evaluating cybersecurity personnel for hire, and adopt a hierarchy of management, who is aware of the standards of cybersecurity in the workplace. Such management should be aware of the value of utilizing the NICE Framework published by the National Institute of Standards and Technology under SP 800-181, Rev. 1- Workforce Framework for Cybersecurity. This medium outlines roles and responsibilities for each level of cybersecurity workforce personnel and explains how these practitioners must align their actions and behavior with their role as cybersecurity leader. Unless this approach is enacted, institutions of higher education will stagnate in deploying updated efforts and strategies to cultivate a cybersecurity culture, employees' will honor and align their behavior with.

Usage of an assessment of all cybersecurity personnel, executive leaders, administrators, faculty, and staff, regarding their role, responsibilities, and acceptable human behavior in the workplace culture, to enhance awareness of cyber-attack incidents, must be implemented. This method must be evaluated bi-annually to update training methods and tool designs that help assess levels of competency in adhering to each cybersecurity policy and information security policy adopted, installed, and relied on as cybersecurity leadership. Assessments must be recorded to determine the scale of commitment each employee has towards accepting cybersecurity awareness training as well as score each employees' attitude about compliance with each policy type. In doing so, the institution can define its approach to motivating employees attitude towards compliance.

Increased reliance on cloud computing storage has become beneficial in reducing access to sensitive data assets. Partnering with a reliable third-party service and product provider will be key in developing usage of this storage system. However, all cybersecurity personnel must be trained to understand the cloud computing system relied on as well as know how to develop the architect for all storage components, including EC2 instances, policies, system configurations, and multi-authentication access controls. This includes having the knowledge to maintain written logs, understanding how to update system configurations as the system scales up or down, and understand what laws the service provider should be aligning their Service Level Agreements with, to ensure the services are secured and

impenetrable. Thus, additional training must be rendered through the institution and the service provider, to ensure each practitioner remains knowledgeable of all system operations, configurations, and security settings.

Updates must be applied to all software and hardware applications, tools, and devices. Such updates should be controlled by written logs that include name of practitioner that deployed the update, date and time stamp must be provided when updates are deployed, and a quarterly report must be shared with executive leaders to communicate what is being done regularly to ensure system security is effective. This also must include providing verbal presentations to executive leaders to discuss any needed technology software and hardware that can enhance security levels and controls, as well as provide clearly conveyed analytic reports. Usage of artificial intelligence for automation can be utilized, but these systems and applications must be configured correctly, monitored effectively, and secured consistently. Reliance on automation of third-party entity service and product providers can be a daunting task when institutions of higher education neglect to stay current in their assessment of their networks, hardware, software, and cloud systems.

Back-up and archive of all networks and information systems is mandatory! Neglecting to do so can be costly. Failure to back-up files can result in system depilation and deterioration of secure applications when cybercriminal breach. This means, institutions of higher education must ensure their systems are consistently backed-up and archived. Multi-factor authentication must be consistent and updated regularly to ensure heightened encryption is applied effectively. Training must be provided to each cybersecurity personnel to ensure each personnel remains knowledgeable of what is required to maintain exclusive security on the system and all its applications. Neglecting to do so will create an entrance point for threats and vulnerabilities to become exploitable.

Adhering to all federal laws, state laws, and international laws is mandatory! This means, all cybersecurity leaders must be aware of what they are held accountable too, as well as know how to adopt policy recommendations and integrate them in the policy outlines of their institution. Doing so can ensure increased development of policy that remain current with trends in technology, software, hardware, cloud computing, and artificial intelligence useful in supporting the security of information assets in networks and cloud computing storage. Network intrusion detection and intrusion prevention must be utilized. Reports must be maintained to ensure these systems are current, configured correctly, and are effective in notifying network administrators regarding alarms that do not align with baselines. Partnering with federal organizations to help create training is essential. When these partnerships are formulated, it can enhance the scale of knowledge sharing and security applied across the institution.

Executive leaders, administrators, faculty, and staff must be trained consistently to be made aware of the risk woven in the technology tools and applications relied on. Training should provide declarative information that is current and clearly written, and easy to adapt and understand. Technical jargon should be omitted, and content should be delivered in English, unless the learners are of other languages. Even then, content should meet the language barriers of all learners to be effective.

All policies must be assessed, developed, implemented, and updated regularly. All policies must be easy to read. All policies must be conveyed with definitions and lists of abbreviations when applicable. All policies must be effective in training end-users to comply. All policies must be without error in grammar, spelling, punctuation, and sentence structure, to be understood in alignment with the American Psychology Association standards in scholarly writing and authorship.

In conclusion, it has been evaluated and research proves cybersecurity leadership is a dynamic approach to controlling threats and vulnerabilities in software and hardware applications, tools, and devices. It has also been proven that usage of cybersecurity policy and information security policy can improve how institutions of higher education thwart and deter cyber-attacks. When organizations adhere to federal law and policy regarding cybersecurity leadership that can be achieved through effective development of policy and implementation of such, helps reduce the threat of successful cyber-attack incidents. When an institution of higher education lacks effective cybersecurity leadership and usage of cybersecurity policy, it represents a weakness in determining the scope of cyber deterrence. When deterrence is absent, victimization is successful. Thus, consistency of practice and assessment of actions and activity engulfing human behavior is required to govern the development and implementation of cybersecurity policy as a method of deterrence and thwarting cyber-attack incidents. Ignoring the scope of consistent reports published regarding cybersecurity incidents at higher education institutions in the United States, Europe, and Middle East, is a willful threat to the security of any institution of higher education and its sensitive data assets, and national security.

Compliance with Ethical Standards

Acknowledgements

A special "Thank You" is extended to Dr. Ian McAndrew, former Dean of Doctoral Studies at Capitol Technology University for his consistent support and professionalism. I also extend a special thank you to Dr. Mary Aiken, Dr. Rich, Dr. Shaw, and Dr. Maranga for their due diligence in supporting life-long-learners. Additionally, I thank Capitol Technology University, University of Arizona Global Campus, University of Maryland Global Campus, University of Phoenix, American Public University System, and Bellevue University for rendering the quality education I attained to soar as an expert in my fields of study.

References

[1] Joint Task Force Transformation Initiative. (2020, December 10). Security and privacy controls for federal information systems and organizations. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

[2] Data Breaches Cost Higher Education and Training Organizations $3.7M on average in 2023. https://www.highereddive.com/news/data-breaches-cost-higher-education-colleges/689499/

[3] Miller, E. (2022, September 20). The State of Higher Education Cybersecurity: Top Insights and Trends. https://www.bitlyft.com/resources/the-state-of-higher-education-cybersecurity-insights-trends

[4] Khan, N.S. (2014, October 22). Qualitative research method: grounded theory. https://www.researchgate.net/publication/287400872_Qualitative_Research_Method_Grounded_Theory

[5] Delve, Ho, L & Limpaecher, A. (2021, September 17). The practical guide to grounded theory. Practical guide to grounded theory research. https://delvetool.com/groundedtheory

[6] Ali, F.R., Dominic, D.D.P., Ali, A.E.S., Rehman, M, & Sohail, A. (2021, April 9). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. https://doi.org/10.3390/app11083383

[7] Gouveia, A. & Mullinger, M. (2024, May 7). SOC 2 compliance: the complete introduction. https://www.auditboard.com/blog/soc-2-framework-guide-the-complete-introduction/

[8] Mohajan, D. & Mohajan, K.H. (2022, December 26). Classic grounded theory: A qualitative research on human behavior. https://www.researchgate.net/publication/366593525

[9] National Forum on Education Statistics, (2004, April 30). Forum guide to protecting the privacy of student information. https://nces.ed.gov/pubs2004/privacy/section_6faq.asp#:~:text=of%20confidential%20information%3F-,A.,that%20has%20violated%20the%20law.

[10] National Center for Education Statistics, (2023, July 26). Nearly three-quarters of undergraduates received some type of financial aid in 2019-2020. https://nces.ed.gov/whatsnew/press_releases/7_26_2023.asp

[11] Viano, A. (2024, March 17). Cyberattacks on higher ed rose dramatically last year, the report shows. https://edtechmagazine.com/higher/article/2024/03/cyberattacks-higher-ed-rose-dramatically-last-year-report-shows

[12] Schwartz, N. (2023, August 1). Data breaches cost higher education and training organizations $3.7M on average in 2023. https://www.highereddive.com/news/data-breaches-cost-higher-education-colleges/689499/

[13] Jorstad, A. J. (2024, March 14). Opinion: cyber siege on U.S. industries threatens higher ed. https://www.govtech.com/education/higher-ed/opinion-cyber-seige

[14] Thompson, R. (2023, February). Further and higher education institutions suffer weekly cyber-attacks. https://www.nwcrc.co.uk/post/further-and-higher-education-institutions-suffer-weekly-cyber-attacks

[15] Joint Task Force, (2020, September). Security and privacy controls for information systems and organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[16] Alotaibi, M., Clarke, L.N. & Furnell, S. (2016, December). Information security policies: a review of challenges and influencing factors.

https://www.researchgate.net/publication/313804253_Information_security_policies_A_review_of_challenges_and_influencing_factors

[17] Alhumud, A.A.T., Omar, A. & Altohami, A.M.W. (2023, September 26). An assessment of cybersecurity performance in the Saudis universities: A total quality management approach. https://www.tandfonline.com/doi/epdf/10.1080/2331186X.2023.2265227?needAccess=true

[18] U.S. GAO Watch Blog, (2024, January) As cyberattacks increase on K-12 schools, here Is what's being done. https://www.cosn.org/wp-content/uploads/2024/01/CoSN-Cybersecurity-Policy-Developments-2023.pdf